ID: 518864
Sample Name: fbXTgwatuJ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:54:25
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

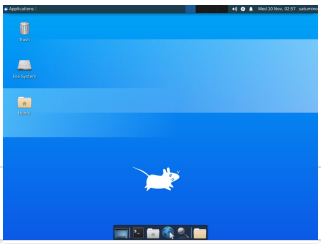
Linux Analysis Report fbXTgwatuJ

Overview

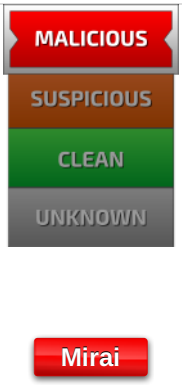
General Information

Sample Name:	fbXTgwatuJ
Analysis ID:	518864
MD5:	24f322c83a02e56.
SHA1:	f60f06d2c600694..
SHA256:	bd1499d689ff1b6..
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

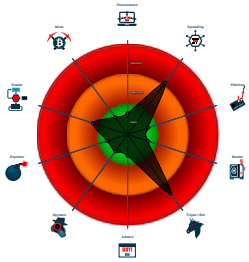


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- Connects to many ports of the same...
- Sample has stripped symbol table
- HTTP GET or POST without a user ...
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	518864
Start date:	10.11.2021
Start time:	02:54:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fbXTgwatuJ
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal76.spre.troj.lin@0/2@0/0
Warnings:	Show All

Process Tree

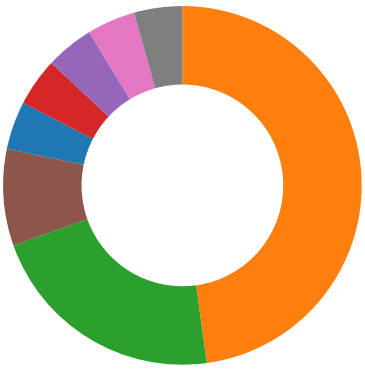
- **system is lnxubuntu20**
- fbXTgwatuJ (PID: 5221, Parent: 5117, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/fbXTgwatuJ
  - fbXTgwatuJ New Fork (PID: 5240, Parent: 5221)
  - fbXTgwatuJ New Fork (PID: 5241, Parent: 5221)
  - fbXTgwatuJ New Fork (PID: 5242, Parent: 5221)
    - fbXTgwatuJ New Fork (PID: 5246, Parent: 5242)
    - fbXTgwatuJ New Fork (PID: 5247, Parent: 5242)
    - fbXTgwatuJ New Fork (PID: 5249, Parent: 5242)
    - fbXTgwatuJ New Fork (PID: 5253, Parent: 5242)
    - fbXTgwatuJ New Fork (PID: 5254, Parent: 5242)
- systemd New Fork (PID: 5273, Parent: 1)
  - sshd (PID: 5273, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5274, Parent: 1)
  - sshd (PID: 5274, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Connects to many ports of the same IP (likely port scanning)

System Summary:

Sample tries to kill many processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

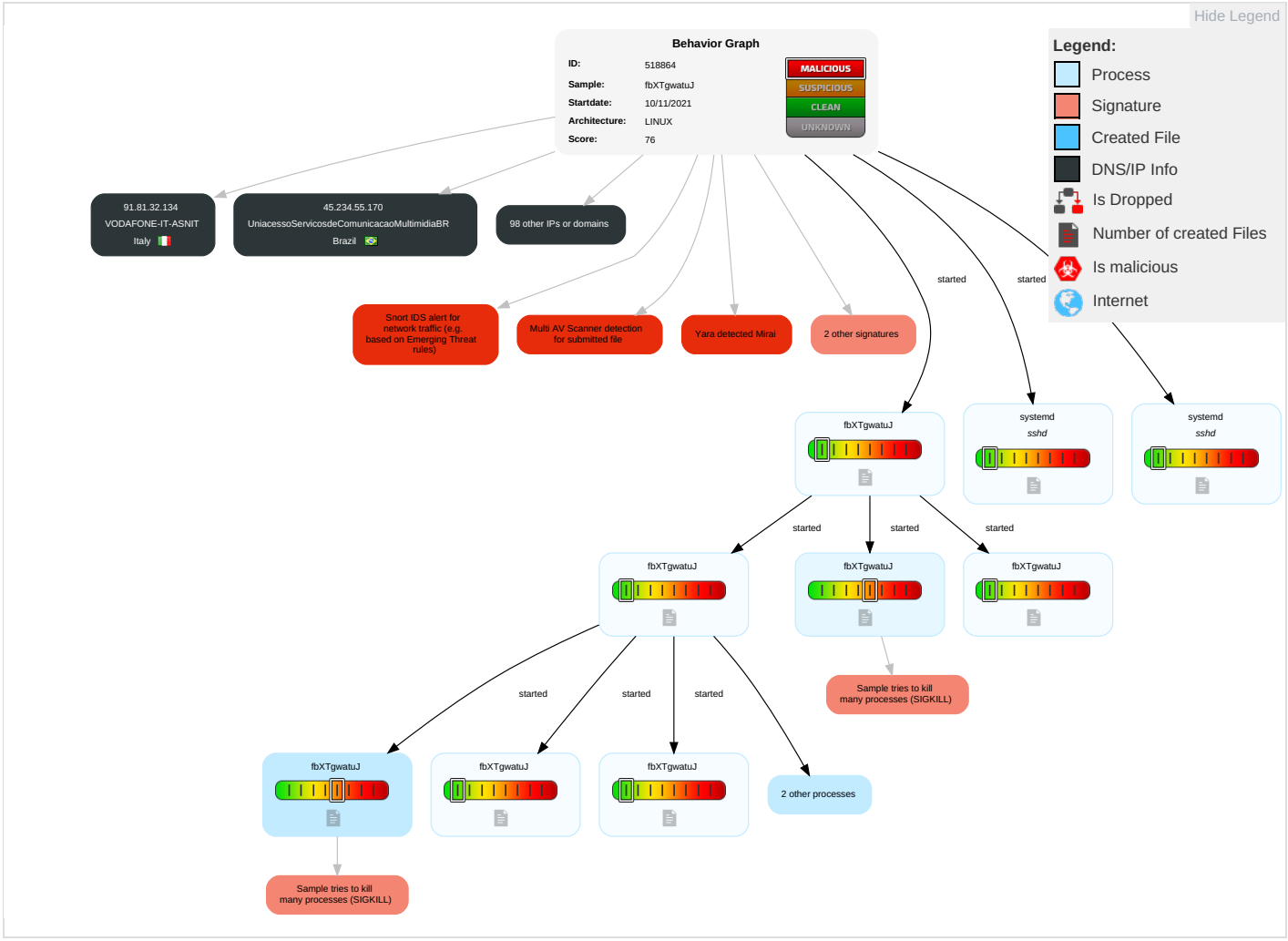
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

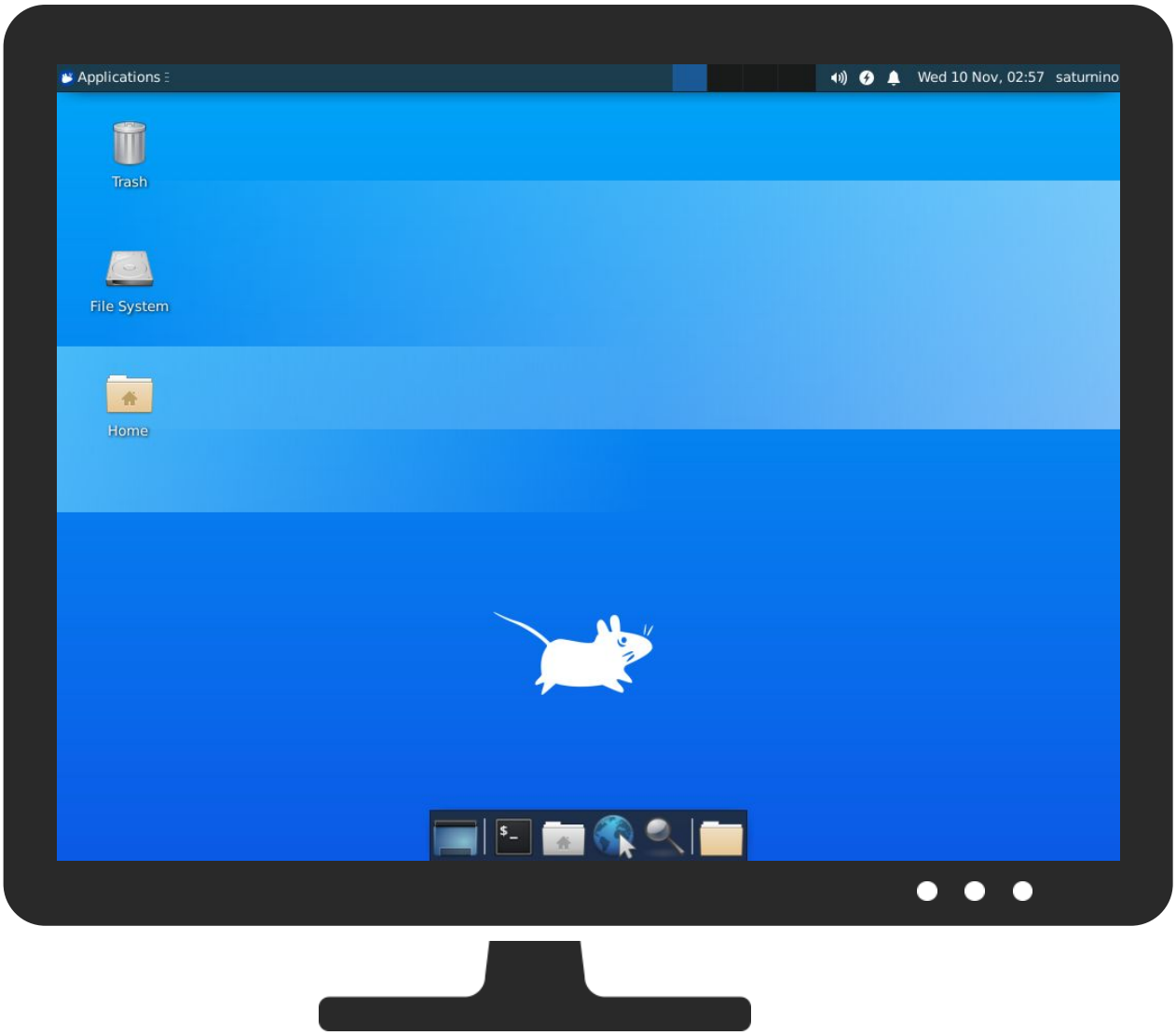
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
fbXTgwatuJ	59%	Virustotal		Browse
fbXTgwatuJ	51%	Metadefender		Browse
fbXTgwatuJ	71%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://103.3.246.123/bins/Hilix.mips	14%	Virustotal		Browse
http://103.3.246.123/bins/Hilix.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.222.232.192	unknown	Ghana		37282	MAINONENG	false
43.148.246.116	unknown	Japan		4249	LILLY-ASUS	false
13.225.123.90	unknown	United States		16509	AMAZON-02US	false
123.81.9.213	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
185.252.217.161	unknown	Germany		12460	MANDALA-ASDE	false
197.166.142.70	unknown	Egypt		24863	LINKdotNET-ASEG	false
185.106.143.21	unknown	Serbia		7979	SERVERS-COMUS	false
197.49.247.206	unknown	Egypt		8452	TE-ASTE-ASEG	false
129.45.93.101	unknown	Algeria		327931	Optimum-Telecom-AlgeriaDZ	false
185.176.0.86	unknown	Ireland		47720	CIX-ASIE	false
136.151.234.158	unknown	United States		1204	SUNYNET-ASN-ASUS	false
91.222.6.78	unknown	Serbia		51859	MNSHA-ASRS	false
185.24.218.206	unknown	Poland		59491	LIVENET-PL	false
67.165.175.121	unknown	United States		7922	COMCAST-7922US	false
41.163.216.170	unknown	South Africa		36937	Neotel-ASZA	false
53.12.120.130	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
2.198.34.2	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
91.244.134.28	unknown	Ukraine		44798	PERVOMAYSK-ASUA	false
45.243.90.255	unknown	Egypt		24863	LINKdotNET-ASEG	false
44.78.196.125	unknown	United States		7377	UCSDUS	false
45.239.81.159	unknown	Brazil		268384	JCTELECOMBR	false
91.180.11.220	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
41.203.40.70	unknown	South Africa		36968	ECN-AS1ZA	false
156.204.73.129	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.96.114.31	unknown	Egypt		37069	MOBINILEG	false
159.214.148.103	unknown	United States		10953	PECOUS	false
145.117.49.194	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
185.78.207.83	unknown	United Kingdom		8426	CLARANET-ASClaraNETLTDGB	false
156.193.176.230	unknown	Egypt		8452	TE-ASTE-ASEG	false
91.19.4.104	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
12.32.255.219	unknown	United States		2386	INS-ASUS	false
91.214.40.193	unknown	Russian Federation		60684	BNEDV-NETRU	false
45.153.14.23	unknown	Russian Federation		208221	ORIONNET-BRKRU	false
45.111.113.76	unknown	Egypt		37069	MOBINILEG	false
197.224.41.156	unknown	Mauritius		23889	MauritiusTelecomMU	false
185.41.67.136	unknown	Norway		50272	AVURAVURNO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.2.167.112	unknown	Canada		7311	FRONTIERCA	false
45.159.66.144	unknown	Italy		60917	TEDRATEDRABACKBONEES	false
185.134.76.10	unknown	Luxembourg		50754	C2DLU	false
44.190.185.40	unknown	United States		39702	SIT-ASDE	false
91.156.132.81	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
220.143.72.166	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
185.15.125.98	unknown	Denmark		208237	AS_NKKOMDK	false
91.209.253.76	unknown	Saudi Arabia		48701	CABASPS	false
185.199.219.198	unknown	Germany		41955	SERNETSerNetServiceNetworkGmbHGoettingenDE	false
197.116.147.40	unknown	Algeria		36947	ALGTEL-ASDZ	false
74.210.198.233	unknown	Canada		11290	CC-3272CA	false
41.148.201.194	unknown	South Africa		5713	SAIX-NETZA	false
91.125.23.8	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
45.190.8.43	unknown	unknown		269617	SolutionsTelecomProvedoredeInternetLTDA-MEBR	false
91.0.244.23	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
197.120.220.102	unknown	Egypt		36992	ETISALAT-MISREG	false
45.25.228.40	unknown	United States		7018	ATT-INTERNET4US	false
45.102.218.5	unknown	Egypt		37069	MOBINILEG	false
156.143.35.216	unknown	United States		14319	FURMAN-2US	false
70.207.197.16	unknown	United States		22394	CELLCOUS	false
91.53.232.18	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
50.180.82.50	unknown	United States		7922	COMCAST-7922US	false
41.221.211.177	unknown	South Africa		3491	BTN-ASNUS	false
41.39.124.196	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.124.0.180	unknown	United Kingdom		204085	NGSGB	false
91.254.252.147	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
66.121.87.98	unknown	United States		7132	SBIS-ASUS	false
185.22.127.130	unknown	Czech Republic		33883	TRIONET-CZ-ASNIXCZ	false
45.234.55.170	unknown	Brazil		267360	UniacessoServicosdeComunicacaoMultimidiaBR	false
91.219.76.51	unknown	Netherlands		51571	PROTECHNICSNL	false
185.240.220.103	unknown	Czech Republic		204772	RSD-CZ	false
156.199.251.111	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.96.114.49	unknown	Egypt		37069	MOBINILEG	false
45.223.169.231	unknown	United States		327849	ROCKETNETZA	false
45.252.226.223	unknown	China		132116	ANINETWORK-INAniNetworkPvtLtdIN	false
113.204.87.244	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
45.141.18.12	unknown	Netherlands		34562	PROIP-ASIncaseofproblemscontactnocproipnetNL	false
185.246.190.10	unknown	Romania		3164	ASTIMPRO	false
37.69.111.68	unknown	France		15557	LDCOMNETFR	false
40.111.155.130	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
91.0.208.216	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.248.153.194	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
23.129.169.180	unknown	Reserved		46723	RESNETUS	false
17.135.215.183	unknown	United States		714	APPLE-ENGINEERINGUS	false
59.215.60.179	unknown	China		2516	KDDIKDDICORPORATIONJP	false
91.81.32.134	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
45.187.4.117	unknown	unknown		269846	TVZAMORACAVE	false
91.244.56.37	unknown	Ukraine		25133	MCLAUT-ASUA	false
222.182.208.77	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
135.33.188.37	unknown	United States		54614	CIKTELECOM-CABLECA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.231.215.252	unknown	Germany		204965	MED360GRADDE	false
91.223.43.9	unknown	Slovenia		199612	BISNODESI	false
111.16.37.200	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
156.99.130.87	unknown	United States		1998	STATE-OF-MNUS	false
45.224.65.234	unknown	Brazil		266916	MARCIOCARDOSOFAGUNDESMEBR	false
155.117.235.41	unknown	United States		11003	PANDGUS	false
91.106.162.52	unknown	Germany		198930	DE-VSM-ASNPeeringDE	false
91.169.219.34	unknown	France		12322	PROXADFR	false
128.10.87.105	unknown	United States		17	PURDUEUS	false
75.190.128.227	unknown	United States		11426	TWC-11426-CAROLINASUS	false
156.79.92.14	unknown	United States		11363	FUJITSU-USAUS	false
91.193.176.179	unknown	Russian Federation		16345	BEE-ASRussiaRU	false
185.184.141.169	unknown	United Kingdom		52423	DataMinersSARacknationcrCR	false
212.153.127.43	unknown	Netherlands		702	UUNETUS	false

Runtime Messages

Command:	/tmp/fbXTgwatuJ
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.180.11.220	SCahhGpqlT	Get hash	malicious	Browse	
91.222.6.78	UguI8hPCWh	Get hash	malicious	Browse	
41.163.216.170	qKjg35J4FG	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MAINONENG	Zhh51946Eq	Get hash	malicious	Browse	• 45.222.232.178
	x86_64	Get hash	malicious	Browse	• 45.222.232.179
	LOF3X5rpl9	Get hash	malicious	Browse	• 154.113.68.238
	jew.x86	Get hash	malicious	Browse	• 197.253.55.177
	sora.x86	Get hash	malicious	Browse	• 45.222.248.93
	QUqBgpQj3B	Get hash	malicious	Browse	• 45.222.232.189
	8pAbCU5dKP	Get hash	malicious	Browse	• 154.113.177.204
	8kNgpvKpMy	Get hash	malicious	Browse	• 154.113.68.244
AMAZON-02US	27xJuvcfMM	Get hash	malicious	Browse	• 54.250.225.134
	E4438FE55AD506189992ED8BFA402449106E5C7D0AE3A.exe	Get hash	malicious	Browse	• 3.13.191.225
	rEOqCaa9fM.apk	Get hash	malicious	Browse	• 52.92.163.216
	Passcode_for_jsartori_451_6.html	Get hash	malicious	Browse	• 52.34.207.165
	DevInstallerBeta.exe	Get hash	malicious	Browse	• 104.192.141.1
	DevInstallerBeta.exe	Get hash	malicious	Browse	• 52.217.129.129

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Devoncs-Attachment 2021-11-09 File - 5849057.html	Get hash	malicious	Browse	• 13.32.219.88
	PO_AMO_8100045923.exe	Get hash	malicious	Browse	• 50.18.238.17
	zuroq8.dll	Get hash	malicious	Browse	• 205.251.242.103
	zuroq1.dll	Get hash	malicious	Browse	• 176.32.103.205
	BSDs-4933.PZTOJFSSIFHXAAYTSKOMYAGCHTHAOF#U00f1.msi	Get hash	malicious	Browse	• 13.249.13.93
	8557527948257.html	Get hash	malicious	Browse	• 13.249.13.23
	SOA & INV FOR OCT'21.exe	Get hash	malicious	Browse	• 3.64.163.50
	Order confirmation.exe	Get hash	malicious	Browse	• 54.176.36.242
	vbc.exe	Get hash	malicious	Browse	• 44.227.65.245
	Vergi #U00f6deme faturas#U0131 9 Kas#U0131m 2021 Sal#U0131,pdf.exe	Get hash	malicious	Browse	• 75.2.115.196
	MV OCEANLADY.docx	Get hash	malicious	Browse	• 76.223.86.4
	PO#SC83994.docx	Get hash	malicious	Browse	• 76.223.86.4
	PO_SC83994.docx	Get hash	malicious	Browse	• 13.248.219.100
	mips	Get hash	malicious	Browse	• 13.52.84.58
LILLY-ASUS	27xJuvcfMM	Get hash	malicious	Browse	• 43.51.1.174
	PO03112021STK#Approved#.exe	Get hash	malicious	Browse	• 43.128.51.206
	mips	Get hash	malicious	Browse	• 40.195.110.117
	x86_64	Get hash	malicious	Browse	• 42.214.198.198
	arm	Get hash	malicious	Browse	• 43.220.27.140
	arm5	Get hash	malicious	Browse	• 42.211.12.113
	Quote request.exe	Get hash	malicious	Browse	• 43.132.183.85
	GB0O1NUtmJ	Get hash	malicious	Browse	• 43.168.211.141
	4DrtSJOLjr	Get hash	malicious	Browse	• 40.22.172.35
	LAQh74RNEl	Get hash	malicious	Browse	• 40.15.158.75
	Kz2SeJpaxw	Get hash	malicious	Browse	• 43.61.74.28
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 40.2.50.69
	BKyU0T5xcw	Get hash	malicious	Browse	• 43.115.211.129
	ZvUGMRqJrx	Get hash	malicious	Browse	• 40.53.145.123
	jyTZMJKPD2	Get hash	malicious	Browse	• 43.18.191.106
	P8NtIPe7f0	Get hash	malicious	Browse	• 40.41.25.83
	OoeA4dABtV	Get hash	malicious	Browse	• 43.73.22.170
	gFn4iz8ygL	Get hash	malicious	Browse	• 40.16.69.95
	b8xw7rKh8F	Get hash	malicious	Browse	• 43.10.117.153
	SQFoFeC1jQ	Get hash	malicious	Browse	• 43.146.166.26

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5274/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file

/proc/5274/oom_score_adj	
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Civ:CM
MD5:	399A14B7B28E9470E1BE6F272272890A
SHA1:	5B82D7F69C166B978FBFC8009876BE4797BAAC8D
SHA-256:	7C92CC37DF60EBCCC15A4175839687DD0EC20BD8FA9A730DD1C193473D3A5860
SHA-512:	01619BEF8D2ADA8E3EBF14DB84500B3F0D1F8C19AB9FE963C74C39168DB2719E21B8AA033FFA1B6FCE28C07D54B4B098CB5FBB255908170484C683DD1752CBD9
Malicious:	false
Reputation:	low
Preview:	5274.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.519175023882212
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	fbXTgwatuJ
File size:	80052
MD5:	24f322c83a02e56c509deb0f9baf28b4
SHA1:	f60f06d2c600694d5b0446d7a9bc4d85ae25366b
SHA256:	bd1499d689ff1b6cd861b79f18c133709f6bcb118bb07956aa10848d3adac7d7
SHA512:	82694b09a1080aacc78dcd702eacd1d2e3e244df8a2ff1bb4455e65679b51f98489bd2341b32609bbe0dd342d90f8abf5cc2dd7a7e21312ef45d968a1ec6bee
SSDEEP:	1536:aqJw3YsMggETUfX9bBSsZjZbjZXxhaGAbH2D:aqJesZETUPBbjLD
File Content Preview:	.ELF.....`.@.4....6.....4. ...(.....@...@..@-..@-.....0...0E..0E. ...`.....Q.td.....<...'!.....'.....<...'!.. .....9'.. .....<x..'!.....9

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	79492
Section Header Size:	40
Number of Section Headers:	14

ELF header

Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x11a20	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x411b40	0x11b40	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x411ba0	0x11ba0	0x11a0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x453000	0x13000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x453008	0x13008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x453014	0x13014	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x453020	0x13020	0x250	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x453270	0x13270	0x3b0	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x453620	0x13620	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x453650	0x13620	0x310	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x6d2	0x13620	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x13620	0x64	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x12d40	0x12d40	3.5572	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x13000	0x453000	0x453000	0x620	0x960	2.4507	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: fbXTgwatuJ PID: 5221 Parent PID: 5117

General

Start time:	02:55:04
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	/tmp/fbXTgwatuJ
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: fbXTgwatuJ PID: 5240 Parent PID: 5221

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: fbXTgwatuJ PID: 5241 Parent PID: 5221

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: fbXTgwatuJ PID: 5242 Parent PID: 5221

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: fbXTgwatuJ PID: 5246 Parent PID: 5242

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: fbXTgwatuJ PID: 5247 Parent PID: 5242

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: fbXTgwatuJ PID: 5249 Parent PID: 5242

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: fbXTgwatuJ PID: 5253 Parent PID: 5242

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: fbXTgwatuJ PID: 5254 Parent PID: 5242

General

Start time:	02:55:05
Start date:	10/11/2021
Path:	/tmp/fbXTgwatuJ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: systemd PID: 5273 Parent PID: 1

General

Start time:	02:55:16
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5273 Parent PID: 1

General

Start time:	02:55:16
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5274 Parent PID: 1

General

Start time:	02:55:16
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5274 Parent PID: 1

General

Start time:	02:55:16
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated